

AMENDMENTS TO THE ABSTRACT

Please delete the section entitled “ABSTRACT OF THE DISCLOSURE” in its entirety and substitute the following section therefor:

ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction, OFB mode logic, and execution logic. The cryptographic instruction is received by a pipeline microprocessor as part of an application program executing on the pipeline microprocessor. The cryptographic instruction prescribes one of the cryptographic operations. The one of the cryptographic operations includes a plurality of OFB block cryptographic operations performed on a corresponding plurality of input text blocks. The OFB mode logic is operatively coupled to the cryptographic instruction. The OFB mode logic directs the pipeline microprocessor to update pointer registers and an initialization vector location for each of the plurality of CFB block cryptographic operations. The execution logic is operatively coupled to the OFB mode logic. The execution logic executes the one of the cryptographic operations.